



Daily Open Source Infrastructure Report 05 March 2015

Top Stories

- California officials stopped production at 12 wells used to pump oil-and-gas in Central Valley March 3 in order to protect underground drinking-water from contamination. – *Associated Press* (See item [1](#))
- A former correctional officer was arrested and charged March 3 in connection to two separate shooting incidents including one on the Maryland Intercounty Connector, and a second incident where shots were fired near the NSA headquarters in Fort Meade. – *WRC 4 Washington, D.C.* (See item [13](#))
- A vulnerability dubbed FREAK was found in the implementation of secure sockets layer (SSL) and transport layer security (TLS) protocols on Apple and Android devices that can be abused through man-in-the-middle (MitM). – *Softpedia* (See item [20](#))
- Four suspects were charged March 3 in connection to more than 40 crash-and-grab thefts netting over \$2 million across Chicago and other areas of the Midwest since 2014. – *Chicago Sun-Times* (See item [24](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

1. *March 4, Associated Press* – (California) **California shuts down oil wells to protect ground water.** The California Department of Conservation stopped production at 12 wells used to pump oil-and-gas in Central Valley March 3 in order to protect underground drinking-water from contamination following a review that found over 2,500 instances when the State authorized the injection of oilfield waste into protected aquifers used for drinking water or irrigating crops. Two operators were issued cease-and-desist orders while 10 other oil wells in Kern County stopped production.
Source: <http://www.nbcbayarea.com/news/california/California-Shuts-Down-Oil-Wells-to-Protect-Ground-Water-294933891.html>
2. *March 4, WTVC 9 Chattanooga* – (Tennessee) **Dozens of customers still without power a week after ice storm.** Volunteer Energy Cooperative reported March 4 that crews continued work to restore service to the remaining 132 customers in Tennessee following an ice storm that knocked out power to about 40,000 customers, broke over 700 poles, caused a loss of power to at least 5 substations, and left an estimated \$9.5 million in damage to the system.
Source: <http://www.newschannel9.com/news/top-stories/stories/dozens-customers-still-without-power-week-after-ice-storm-15574.shtml>

[\[Return to top\]](#)

Chemical Industry Sector

Nothing to report

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

3. *March 3, WREX 13 Rockford* – (Illinois) **‘Chunk of ice’ shuts down Unit 1 at Byron nuclear power plant.** Exelon Corporation officials announced that an automatic shutdown of the Unit 1 reactor at the Byron Generating Station in Ogle County, Illinois, March 3 was likely caused by a large chunk of ice that interrupted power to the unit. The shutdown did not affect local service to customers, and crews are making the necessary repairs.
Source: <http://www.wrex.com/story/28253184/2015/03/03/chunk-of-ice-shuts-down-unit-1-at-byron-nuclear-power-plant>

[\[Return to top\]](#)

Critical Manufacturing Sector

Nothing to report

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Financial Services Sector

4. *March 3, Softpedia* – (International) **Banking malware targets almost 1,500 financial institutions in 86 countries.** Security researchers from Symantec reported an analysis of 999 banking malware configurations that targeted 1,467 financial institutions worldwide in 2014, most of which were in the U.S. where consumers have been attacked with 95 percent of the trojans analyzed. The analysis also revealed that 4.1 million users' systems had been compromised in 2014.
Source: <http://news.softpedia.com/news/Banking-Malware-Targets-Almost-1-500-Financial-Institutions-in-86-Countries-474782.shtml>
5. *March 3, Threatpost* – (International) **New POS malware uses mailslots to avoid detection.** Security researchers from Morphick discovered that the new LogPOS point-of-sale (PoS) malware uses Microsoft Windows' mailslots technology to avoid detection. inject code, and act like a client while it relays stolen payment card numbers to a command and control (C&C) server.
Source: <http://threatpost.com/new-pos-malware-uses-mailslots-to-avoid-detection/111391>

For another story, see item [20](#)

[\[Return to top\]](#)

Transportation Systems Sector

6. *March 4, Santa Cruz Sentinel* – (California) **Santa Cruz: Six protestors who blocked Highway 1 arrested.** Southbound Highway 1 in Santa Cruz reopened after being closed for 5 hours due to University of California, Santa Cruz student protestors who chained themselves to bins filled with 700 pounds of concrete and blocked the roadway March 3. Authorities arrested six students before clearing the highway to reopen.
Source: http://www.mercurynews.com/central-coast/ci_27633502/santa-cruz-protesters-block-highway-1-slow-highway
7. *March 3, WSYX 6 Columbus* – (Ohio) **I-70 reopens after fertilizer spill closed lanes for hours.** Westbound lanes of Interstate 70 near Livingston Avenue in Ohio reopened after being closed for nearly 4 hours March 3 while crews cleared a fertilizer spill.
Source: <http://www.abc6onyourside.com/news/features/top-stories/stories/Update-I-70-Reopens-After-Fertilizer-Spill-Closed-Lanes-For-Hours-98201.shtml>
8. *March 3, St. Cloud Times* – (Minnesota) **All lanes of I-94 open after collisions near Clearwater.** The Minnesota Department of Transportation reported that all lanes of

Interstate Highway 94 in St. Cloud reopened after being closed for nearly 4 hours March 3 due to 31 collisions that caused injuries following heavy snow fall.

Source: <http://www.sctimes.com/story/news/local/2015/03/03/interstate-near-clearwater-closed-traffic/24311173/>

9. *March 2, CNN* – (National) **Report: Air traffic control system vulnerable to cyberattack.** The U.S. Government Accountability Office (GAO) released a report March 2 claiming that the Federal Aviation Administration (FAA) needed to continue addressing significant security control vulnerabilities regarding its cyber-security measures that continue to threaten the agency's ability to ensure safe and uninterrupted operation of the national space system. The FAA reportedly agreed with GAO's recommendations for improvement and stated that the agency was working towards increasing cyber-security.
Source: <http://www.cnn.com/2015/03/02/politics/cyberattack-faa-air-traffic-control-hacking/>

For another story, see item [13](#)

[\[Return to top\]](#)

Food and Agriculture Sector

10. *March 4, U.S. Food and Drug Administration* – (National) **Maternal Science, Inc. issues allergy alert on undeclared milk in healthy mama Boost It Up!; mango drink.** The U.S. Food and Drug Administration reported March 3 that Maternal Science, Inc., voluntarily issued a recall for its healthy mama Boost It Up! mango drinks due to undeclared whey protein isolate (milk). The recalled products were packaged in 12-ounce bottles and were sold nationwide through limited retailers and via Internet sales.
Source: <http://www.fda.gov/Safety/Recalls/ucm436491.htm>
11. *March 3, Canandaigua Daily Messenger* – (New York) **Unstable roof shuts down Pactiv operations.** A potential roof collapse at the Pactiv Corporation food service and food manufacturing facility in Canandaigua, New York, March 3 prompted the evacuation of at least one building as water drained into the high-security plant. Operations at the facility were halted until further notice while crews investigated and worked to contain the damage.
Source: <http://www.mpnnow.com/article/20150303/NEWS/150309862/1994/NEWS>
12. *March 3, KRGV 5 Weslaco* – (Texas) **Family farm must shutdown citrus operation due to fruit fly.** The U.S. Department of Agriculture (USDA) imposed a 1 square mile quarantine in Brownsville, Texas, that will last through May and halted sales from a citrus operation at Loop Farms after USDA agents detected an invasive Mexican fruit fly on a residential tree in the area. The temporary shutdown of the commercial grove is estimated to cost between \$15,000 and \$20,000 in lost citrus sales.
Source: <http://www.krgv.com/news/local-news/Family-Farm-Must-Shutdown-Citrus-Operation-Due-to-Fruit-Fly/31597140>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

See item [1](#)

[\[Return to top\]](#)

Healthcare and Public Health Sector

See item [16](#)

[\[Return to top\]](#)

Government Facilities Sector

13. *March 4, WRC 4 Washington, D.C.* – (Maryland; Washington, D.C.) **Former correctional officer charged in shootings at NSA, ICC.** A former correctional officer was arrested and charged March 3 in connection to two separate shooting incidents, including one on the Maryland Intercounty Connector near Interstate 95 where two individuals were struck by bullets, and a second incident where shots were fired near the NSA headquarters in Fort Meade where a building was damaged. Authorities are investigating if the suspect is connected to a series of other shootings in the Washington, D.C. and Baltimore areas beginning February 24 targeting individuals at shopping centers, a Walmart, and an AMC Theater.
Source: <http://www.nbcwashington.com/news/local/Shots-Fired-Near-NSA-Headquarters-294909111.html>
14. *March 4, Dallas Morning News* – (Texas) **Carbon monoxide leak closes Lakewood Elementary on Wednesday.** Lakewood Elementary School in Dallas remained closed March 4 after high levels of carbon monoxide was detected in the building causing 11 students and 3 staff members to report feeling ill March 2, and prompting an evacuation March 3. Officials found that a dead owl stuck in the ventilation system was the cause of the carbon monoxide buildup.
Source: <http://thescoopblog.dallasnews.com/2015/03/lakewood-elementary-in-dallas-evacuated-over-carbon-monoxide-in-building.html/>
15. *March 3, WNYT 13 Albany* – (New York) **Cohoes City Hall closed; mayor awaits asbestos test results.** Several offices in Cohoes City Hall in New York were closed March 3-4 while officials awaited the results of air quality tests conducted in the flood-damaged basement following a February 9 water main rupture. A repair worker reported February 27 of the possibility of asbestos in the basement prompting authorities to hire environmental crews to take samples.
Source: <http://wnyt.com/article/stories/S3723508.shtml>
16. *March 3, Eugene Register-Guard* – (Oregon) **Hundreds vaccinated at UO.** University of Oregon officials reported March 3 that 770 students were vaccinated against

meningococcal disease March 2 following an outbreak that killed 1 student and sickened 3 others at the Eugene university in 2015. Public health officials recommended that nearly 22,000 students and faculty get vaccinated.

Source: <http://registerguard.com/rg/news/local/32827565-75/770-uo-students-get-vaccinated-at-knight-arena.html.csp>

For additional stories, see items [18](#), [20](#), and [23](#)

[\[Return to top\]](#)

Emergency Services Sector

17. *March 4, WHIO 7 Dayton* – (Ohio) **Gas leak closes Clark County Juvenile Center.** The Clark County Juvenile Center in Springfield, Ohio, was closed March 4 due to a gas leak that forced the evacuation of the building March 3. Crews shut off the gas to the building while working to repair the leak after 28 juveniles were either released on electronic monitoring devices or sent to the Clark County Jail.
Source: <http://www.whio.com/news/news/local/gas-leak-closes-clark-county-juvenile-center/nkNJb/>
18. *March 3, Pensacola Today* – (Florida) **Emergency exercise at UWF for first responders.** A full-scale hazardous materials exercise at the University of West Florida in Pensacola is scheduled for March 10, the District 1 Local Emergency Planning Committee announced March 3. During the exercise participants will respond to a mock incident through simulated response and real-time role play.
Source: <http://pensacolatoday.com/2015/03/emergency-exercise-at-uwf-for-first-responders/>
19. *March 3, Associated Press* – (Utah) **Firefighters wake up to smoke in station, then battle blaze.** A March 3 fire at a Salt Lake City Fire Department facility left the second floor with extensive damage and caused smoke inhalation injuries to nine firefighters. Authorities are investigating the cause of the fire while the firefighters were ordered to work out of other stations until repairs are made.
Source: <http://abcnews.go.com/US/wireStory/hospital-checks-firefighters-station-catches-fire-29356593>

[\[Return to top\]](#)

Information Technology Sector

20. *March 4, Softpedia* – (International) **Strong SSL/TLS ciphers downgraded to use weak crypto key in FREAK attack.** A security researcher at INRIA and the Microsoft Research Team identified a serious vulnerability in the implementation of secure sockets layer (SSL) and transport layer security (TLS) protocols on Apple and Android devices that can be abused through man-in-the-middle (MitM) attacks that capitalize on abandoned policies to force the use of weak RSA keys, potentially leaving a wide range of government and other Web sites vulnerable. The researchers

have dubbed the attack FREAK (Factoring RSA Export Keys) and Akamai cloud platform announced that it patched the vulnerability.

Source: <http://news.softpedia.com/news/Strong-SSL-TLS-Ciphers-Downgraded-to-Use-Weak-Crypto-Key-in-FREAK-Attack-474842.shtml>

21. *March 4, Securityweek* – (International) **Google fixes 51 vulnerabilities with release of Chrome 41.** Google addressed 51 security issues and added new apps, extension application program interfaces (APIs), and stability and performance improvements in the release of Google Chrome version 41. The addressed vulnerabilities include 13 high-severity and 6-medium-severity issues discovered by external researchers.

Source: <http://www.securityweek.com/google-fixes-51-vulnerabilities-release-chrome-41>

For additional stories, see items [4](#) and [5](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

22. *March 2, KHQ 6 Spokane* – (Washington) **Homeless man caught stealing \$10,000 in radio equipment.** Police arrested a man March 2 for stealing radio equipment in Quincy from Cherry Creek Radio's KWWW 96.7 FM Wenatchee radio station worth \$10,000 after station personnel notified the utility company when their transmitter went offline.

Source: <http://www.khq.com/story/28243325/homeless-man-caught-stealing-10000-in-radio-equipment>

[\[Return to top\]](#)

Commercial Facilities Sector

23. *March 4, WABC 7 New York City* – (New York) **Barnard dorm fire leads to evacuations.** A 2-alarm fire that started at Ollie's restaurant located inside a Barnard College dormitory in New York City March 3 sparked a series of explosions that blew off the walls of the restaurant rendering it a total loss and injured at least five individuals. About 200 students were evacuated from the dormitory for about 9 hours, and crews were expected to restore heat, water, and gas services to the building March 4.

Source: <http://7online.com/news/barnard-dorm-fire-leads-to-evacuations/543457/>

24. *March 3, Chicago Sun-Times* – (Illinois) **Crash-and-grab suspects nabbed in \$2 million spree.** The Chicago Police Department announced charges March 3 against four suspects who are believed to be part of a theft ring that is responsible for more than 40 crash-and-grab thefts across the city and other areas of the Midwest since 2014. The suspects are accused of stealing more than \$2 million in merchandise and causing more than \$500,000 in damage to businesses.
Source: <http://chicago.suntimes.com/news-chicago/7/71/411528/crash-grab-suspects-nabbed-2-million-spreed>
25. *March 3, KTNV 13 Las Vegas* – (Nevada) **27 people displaced after apartment fire near Eastern and Stewart.** A March 3 fire at the Stewart Plaza Apartments complex in Las Vegas displaced 27 residents and caused an estimated \$50,000 in damage. Investigators reported that the fire which started in a closet appeared to be accidental and may be electrical in nature.
Source: <http://www.jrn.com/ktnv/news/Apartment-unit-catches-fire-near-Eastern-and-Stewart-294828391.html>
26. *March 3, U.S. Department of Labor* – (New Jersey) **Blocked exits, electrical hazards found after worker electrocuted at distribution warehouse in Dayton, N.J.** The Occupational Safety and Health Administration cited Seldat Distribution Inc., for 10 serious violations including electrical hazards following a September 2014 inspection of the company's Dayton, New Jersey, distribution warehouse that was initiated after a worker was electrocuted by an improperly wired, powered conveyer system. Proposed penalties total \$63,000.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=27510
27. *March 1, California State University, Fullerton Daily Titan* – (California) **Fire causes millions of dollars of damage to Dillon's Bar and Grill.** Authorities are investigating a 4-alarm fire that occurred at Dillon's Bar and Grill in Fullerton March 1 that rendered the restaurant a total loss and caused an estimated \$2-3 million in damage. Nearby businesses were evacuated and firefighters cut off power to the area for about 11 hours as a precaution.
Source: <http://www.dailytitan.com/2015/03/fire-causes-millions-of-dollars-of-damage-to-dillons-bar-and-grill/>

For additional stories, see items [13](#) and [20](#)

[\[Return to top\]](#)

Dams Sector

Nothing to report

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.